

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

CLAIMS:

- 1 1. A proactive operating environment that includes a
2 group of proactive servers communicating over a
3 network; each proactive server (PS_i) comprising:
4 a storage that includes a non erasable part that
5 stores at least a public, non proactive related, key
6 V_{start}^I ; said storage further includes an erasable part
7 for storing private and public data; said proactive
8 server is further associated with a discardable one-time
9 private key S_{start}^I that corresponds to said public key
10 V_{start}^I ; said proactive server is further associated with
11 configuration data C ;
12 a processor for providing at least proactive
13 services to applications;
14 the proactive server is associated with a group
15 public proactive key V_{CERT} common to said group of
16 proactive servers and a share S_{CERT}^I of a corresponding
17 private proactive key S_{CERT} ;
18 the processor is operative to invoke initialization
19 procedure for generating restore related information;
20 the processor is further operative to invoke a
21 restore procedure for utilizing at least said public, non
22 proactive related, key V_{start}^I and said restore related
23 information for restoring at least said public proactive
24 key V_{CERT} .
1 2. The system according to Claim 1, wherein said restore
2 procedure is invoked by refresh procedure.

1 3. The system according to Claim 1, wherein said
2 non erasable part of the storage being a ROM memory
3 module.

1 4. The system according to Claim 1, wherein said
2 applications being at least one of the following:
3 Secure logging, Secure end-to-end communication,
4 Timestamping, Certificate authority, Key recovery, Voting,
5 Trading, Database, Operating system, Access control
6 mechanisms, Secure Commerce.

1 5. The system according to Claim 1, wherein said
2 restore related information includes restore related self
3 information.

1 6. The system according to Claim 1, wherein said
2 restore related information includes restore related
3 others' information.

1 7. The system According to Claim 5, wherein said
2 restore related self information includes $M_I = S^I_{start} (V_{cert},$
3 $C)$.

1 8. The system According to Claim 6, wherein said
2 restore related others' information includes $(S_{cert}(M), M)$.

1 9. The system according to Claim 1, wherein said
2 initialization procedure includes:

- 3 (i) input for receiving at least configuration
- 4 data C , public non-proactive related key V^I_{start} and
- 5 discardable one time private key S^I_{start} ;
- 6 (ii) the processor generating a set of keys $S_I(0)$,
- 7 $V_I(0)$, $E_I(0)$, $D_I(0)$;
- 8 (iii) broadcasting said set of keys except $D_I(0)$
- 9 over the network to the rest of the servers

000000 000000 000000

- 10 (1..i-1,i+1..n) in the group, so as to authenticate
- 11 and encrypt the network channel;
- 12 (iv) the processor generating the group public
- 13 proactive key V_{cert} and a share (S^I_{cert}) of
- 14 corresponding private proactive key S_{cert} ;
- 15 (v) the processor generating restore related self
- 16 information that includes $M_I = S^I_{start} (V_{cert}, C)$.
- 17 (vi) discarding the one-time private key S^I_{start} ;
- 18 (vii) broadcasting M_I to all servers in the group,
- 19 and receiving M_j from all respective SP_j servers in
- 20 the group; the processor concatenating said $M_1..M_N$ so
- 21 as to construct M ;
- 22 (viii) the processor generating a joint signature
- 23 ($S_{cert}(M), M$) that forms part of said restore related
- 24 others' information; and
- 25 (ix) broadcasting the joint signature (S_{cert}
- 26 (M), M).

1 10. The system according to Claim 1, wherein

2 said recover procedure includes:

- 3 (i) the processor extracting V^I_{start} ;
- 4 (ii) the processor extracting M_I from M ;
- 5 (iii) the processor constructing V_{cert} by applying
- 6 V^I_{start} to M_I ;
- 7 (iv) the processor validating M by applying V_{cert}
- 8 to the joint signature part($S_{cert}(M)$); if the result
- 9 matches M then the server becomes operational; sending
- 10 M and $S_{cert}(M)$ to all the group servers;
- 11 (v) if, on the other hand, M is invalid, then
- 12 waiting the receipt of another joint signature and
- 13 in response repeating said (ii) to (iv).

1 11. For use in the system of Claim 1, an initialize
2 procedure.

1 12. For use in the system of Claim 1, a restore
2 procedure.

1 13. A method for providing a proactive security in
2 proactive operating environment; the proactive
3 operating environment includes a group of proactive
4 servers communicating over a network; each proactive
5 server (PS_i) comprising:

6 a storage that includes a non erasable part that
7 stores at least a public, non proactive related, key
8 V_{Start}^I ; said storage further includes an erasable part
9 for storing private and public data; said proactive
10 server is further associated with a discardable one-time
11 private key S_{Start}^I that corresponds to said public key
12 V_{Start}^I ; said proactive server is further associated with
13 configuration data C;

14 a processor for providing at least proactive
15 services to applications;

16 the proactive server is associated with a group
17 public proactive key V_{CERT} common to said group of
18 proactive servers and a share S_{CERT}^I of a corresponding
19 private proactive key S_{CERT} ; the method further including:

20 invoking initialization procedure for generating
21 restore related information; and invoking a restore
22 procedure for utilizing at least said public, non
23 proactive related, key V_{Start}^I and said restore related
24 information for restoring at least said public proactive
25 key V_{CERT} .

1 14. The method according to Claim 13, wherein said
2 restore procedure is invoked by refresh procedure.

- 10 (1..i-1,i+1..n) in the group, so as to authenticate
- 11 and encrypt the network channel;
- 12 (iv) generating the group public proactive key V_{Cert}
- 13 and a share (S^I_{CERT}) of corresponding private
- 14 proactive key S_{CERT} ;
- 15 (v) generating restore related self information that
- 16 includes $M_I = S^I_{Start}(V_{Cert}, C)$;
- 17 (vi) discarding the one-time private key S^I_{Start} ;
- 18 (vii) broadcasting M_I to all servers in the group, and
- 19 receiving M_j from all respective SP_j servers in the
- 20 group; the processor concatenating said $M_1..M_N$ so as
- 21 to construct M ;
- 22 (viii) generating a joint signature $(S_{Cert}(M), M)$ that
- 23 forms part of said restore related others'
- 24 information; and
- 25 (ix) broadcasting the joint signature $(S_{Cert}(M), M)$.

1 22. The method according to Claim 13, wherein
2 said recover procedure includes:

- 3 (i) extracting V^I_{Start} ;
- 4 (ii) extracting M_I from M ;
- 5 (iii) constructing V_{Cert} by applying V^I_{Start} to M_I ;
- 6 (iv) validating M by applying V_{Cert} to the joint
- 7 signature part $(S_{Cert}(M))$; if the result matches M then
- 8 the server becomes operational; sending M and S_{Cert}
- 9 (M) to all the group servers;
- 10 (v) if, on the other hand, M is invalid, then
- 11 waiting the receipt of another joint signature and
- 12 in response repeating said (ii) to (iv).

1 23. For use in the method of Claim 13, an initialize
2 procedure.

25. A storage medium storing computer implemented program for providing a proactive security in proactive operating environment; the proactive operating environment includes a group of proactive servers communicating over a network; each proactive server (PS_i) comprising:

a storage that includes a non erasable part that stores at least a public, non proactive related, key V_{start}^I ; said storage further includes an erasable part for storing private and public data; said proactive server is further associated with a discardable one-time private key S_{start}^I that corresponds to said public key V_{start}^I ; said proactive server is further associated with configuration data C;

a processor for providing at least proactive services to applications;

the proactive server is associated with a group public proactive key V_{CERT} common to said group of proactive servers and a share S^I_{CERT} of a corresponding private proactive key S_{CERT} ; the method further including:

invoking initialization procedure for generating restore related information; and invoking a restore procedure for utilizing at least said public, non proactive related, key V_{start} and said restore related information for restoring at least said public proactive key V_{CERT} .